Terms used: **certificate digital credit card** Found **3,970** of **207,474**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Supporting structured credentials and sensitive policies through interoperable strategies for automated trust negotiation
Ting Yu, Marianne Winslett, Kent E. Seamons
February 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 1
Publisher: ACM Press
Full text available: pdf(507.29 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Business and military partners, companies and their customers, and other closely cooperating parties may have a compelling need to conduct sensitive interactions on line, such as accessing each other's local services and other local resources. Automated trust negotiation is an approach to establishing trust between parties so that such interactions can take place, through the use of access control policies that specify what combinations of digital credentials a stranger must disclose to gain acc ...

Keywords: Automated trust negotiation, access control, digital credentials, interoperable strategies

2 Dynamic Access Control: An access control model for dynamic client-side content
Adam Hess, Kent E. Seamons
June 2003 **Proceedings of the eighth ACM symposium on Access control models and technologies SACMAT '03**
Publisher: ACM Press
Full text available: pdf(608.50 KB) Additional Information: full citation, abstract, references, index terms

The focus of access control in client/server environments is on protecting sensitive server resources by determining whether or not a client is authorized to access those resources. The set of resources are usually static, and an access control policy associated with each resource specifies who is authorized to access the resource. In this paper, we turn the traditional client/server access control model on its head, and address how to protect the sensitive content that clients disclose to serve ...

Keywords: access control, authentication, credentials, trust negotiation

3 Content-triggered trust negotiation
Adam Hess, Jason Holt, Jared Jacobson, Kent E. Seamons

August 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 3
Publisher: ACM Press

Full text available: pdf(815.36 KB) Additional Information: full citation, abstract, references, citings, index terms

The focus of access control in client/server environments is on protecting sensitive server resources by determining whether or not a client is authorized to access those resources. The set of resources is usually static, and an access control policy associated with each resource specifies who is authorized to access the resource. In this article, we turn the traditional client/server access control model on its head and address how to protect the sensitive content that clients disclose to and r ...

Keywords: Trust negotiation, access control, authentication, credentials

4 Constructing fair-exchange protocols for E-commerce via distributed computation of RSA signatures

Jung Min Park, Edwin K. P. Chong, Howard Jay Siegel
July 2003 **Proceedings of the twenty-second annual symposium on Principles of distributed computing PODC '03**
Publisher: ACM Press

Full text available: pdf(1.03 MB) Additional Information: full citation, abstract, references, citings, index terms, review

Applications such as e-commerce payment protocols, electronic contract signing, and certified e-mail delivery require that fair exchange be assured. A fair-exchange protocol allows two parties to exchange items in a fair way so that either each party gets the other's item, or neither party does. We describe a novel method of constructing very efficient fair-exchange protocols by distributing the computation of RSA signatures. Specifically, we employ multisignatures based on the RSA-signature sch ...

Keywords: Fair-exchange protocols, RSA signatures, e-commerce, multisignatures, zero-knowledge proofs

5 Secure Data Publishing and Certificate Management: Interoperable strategies in automated trust negotiation

Ting Yu, Marianne Winslett, Kent E. Seamons
November 2001 **Proceedings of the 8th ACM conference on Computer and Communications Security CCS '01**
Publisher: ACM Press

Full text available: pdf(200.92 KB) Additional Information: full citation, abstract, references, citings, index terms

Automated trust negotiation is an approach to establishing trust between strangers through the exchange of digital credentials and the use of access control policies that specify what combinations of credentials a stranger must disclose in order to gain access to each local service or credential. We introduce the concept of a trust negotiation *protocol*, which defines the ordering of messages and the type of information messages will contain. To carry out trust negotiation, a party pairs i ...

6 Separate handles from names on the internet

Michael J. O'Donnell
December 2005 **Communications of the ACM**, Volume 48 Issue 12
Publisher: ACM Press

Full text available: pdf(83.49 KB) Additional Information: full citation, abstract, references, index terms

html(27.14 KB)

The human meaning of domain names attracts conflict over their control, degrading their reliability as permanent handles. Solution: support handles separately from names.

7 Grid Security Framework for Managing the Certificate

Nilar Thein, Thinn Thu Naing

December 2006 **Proceedings of the 2006 IEEE/WIC/ACM International Conference on Web Intelligence WI '06**

Publisher: IEEE Computer Society

Full text available: pdf(189.03 KB) Additional Information: full citation, abstract

The certificate is a central concept in Grid Security Infrastructure authentication. The certificate guarantees the authenticity of the data, thus effectively authenticating the sender. In this paper, we propose a secure certificate authentication framework using Counting Process to interact trusty for Grid users .We intend to apply this approach in secured performance on Grids as well as in grid application for authenticating users, protecting attacks, and recovering failed systems. The main id ...

Keywords: Counting Process, RSA public key, Certificate, Authentication method and Authorization method

8 IT workforce preparation: Industry certification and academic degrees: complementary, or poles apart?

Leo Hitchcock

April 2007 **Proceedings of the 2007 ACM SIGMIS CPR conference on 2007 computer personnel doctoral consortium and research conference: The global information technology workforce SIGMIS-CPR '07**

Publisher: ACM Press

Full text available: pdf(217.38 KB) Additional Information: full citation, abstract, references, index terms

University ICT degrees give students a well-rounded, broad base with which to move into industry. Graduates may however find that without specific product skills many employers may be reluctant to hire them [9]. One method of credentialing for specific products that has become predominant, described as a "parallel universe" [1], and that many advocate as being complementary to and may integrate with academic degrees, is *industry-based certification*. Some however, see industry certifica ...

Keywords: IS research, IT job market, academic curricula, industry certification, industry-based education

9 Authentication: An approach to certificate path discovery in mobile Ad Hoc networks

He Huang, Shyhtsun Felix Wu

October 2003 **Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks SASN '03**

Publisher: ACM Press

Full text available: pdf(146.93 KB) Additional Information: full citation, abstract, references, citings, index terms

Public key certificates prove validity and authenticity of their ownership and possibly other properties. Certificate path discovery is the critical process for public key verification in hierarchical public key infrastructure (PKI) diagrams. This process is conventionally done in centralized public key management system such as central CA or directory. However, in an infrastructure-less environment, such as a mobile ad hoc network, no such central service is present due to network dynamics. Tha ...

Keywords: MANET, certificate path discovery, public key infrastructure, security

10 Use of nested certificates for efficient, dynamic, and trust preserving public key infrastructure

Albert Levi, M. Ufuk Caglayan, Cetin K. Koc
February 2004 **ACM Transactions on Information and System Security (TISSEC)**, Volume 7 Issue 1
Publisher: ACM Press

Full text available: pdf(532.64 KB) Additional Information: full citation, abstract, references, index terms, review

Certification is a common mechanism for authentic public key distribution. In order to obtain a public key, verifiers need to extract a certificate path from a network of certificates, which is called public key infrastructure (PKI), and verify the certificates on this path recursively. This is classical methodology. Nested certification is a novel methodology for efficient certificate path verification. Basic idea is to issue special certificates (called nested certificates) for other certifica ...

Keywords: Digital certificates, key management, nested certificates, public key infrastructure

11 XML security: Certificate validation service using XKMS for computational grid

Namje Park, Kiyoung Moon, Sungwon Sohn
October 2003 **Proceedings of the 2003 ACM workshop on XML security XMLSEC '03**
Publisher: ACM Press

Full text available: pdf(7.01 MB) Additional Information: full citation, abstract, references, index terms

A computational grid is a hardware and software infrastructure capable of providing dependable, consistent, pervasive, and inexpensive access to high-end computational resource. There are many ways to access the resources of a computational grid, each with unique security requirements and implications for both the resource user and the resource provider. Current Grid security Infrastructure using PKI based on SSO. But open grid service Security Infrastructure in Global Grid Forum(GGF) will exten ...

Keywords: GSI, XKMS, XML, XML security, certificate validation, grid, key management, security

12 Using certes to infer client response time at the web server

David Olshefski, Jason Nieh, Dakshi Agrawal
February 2004 **ACM Transactions on Computer Systems (TOCS)**, Volume 22 Issue 1
Publisher: ACM Press

Full text available: pdf(2.30 MB) Additional Information: full citation, abstract, references, citings, index terms

As businesses continue to grow their World Wide Web presence, it is becoming increasingly vital for them to have quantitative measures of the mean client perceived response times of their web services. We present Certes (CliEnt Response Time Estimated by the Server), an online server-based mechanism that allows web servers to estimate mean client perceived response time, as if measured at the client. Certes is based on a model of TCP that quantifies the effect that connection drops have on mean ...

Keywords: Web server, client perceived response time

13 Educator's symposiums: Preparing undergraduate students for Java certification

Ariel Ortiz
October 2003 **Companion of the 18th annual ACM SIGPLAN conference on Object-oriented programming, systems, languages, and applications OOPSLA '03**
Publisher: ACM Press
Full text available: pdf(275.82 KB) Additional Information: full citation, abstract, references, index terms

Java certification promises to make our students more marketable once they graduate. The truth is that certifications in general offer significant advantages, but it is important not to overestimate their benefits. In this paper, we describe our experiences on teaching a workshop aimed at preparing undergraduate students for the Sun Certified Java Programmer exam. But first, we layout the real value of IT certifications and explain the different certification options available for Java technolog ...

Keywords: Java, SCJP, certification

14 Certificate-based authorization policy in a PKI environment

Mary R. Thompson, Abdelilah Essiari, Srilekha Mudumbai
November 2003 **ACM Transactions on Information and System Security (TISSEC)**, Volume 6 Issue 4
Publisher: ACM Press
Full text available: pdf(233.63 KB) Additional Information: full citation, abstract, references, citings, index terms

The major emphasis of public key infrastructure has been to provide a cryptographically secure means of authenticating identities. However, procedures for authorizing the holders of these identities to perform specific actions still need additional research and development. While there are a number of proposed standards for authorization structures and protocols such as KeyNote, SPKI, and SAML based on X.509 or other key-based identities, none have been widely adopted. As part of an effort to us ...

Keywords: Public key infrastructure, XML, digital certificates

15 Large systems: Small worlds in security systems: an analysis of the PGP certificate graph

Srdjan Čapkun, Levente Buttyán, Jean-Pierre Hubaux
September 2002 **Proceedings of the 2002 workshop on New security paradigms NSPW '02**
Publisher: ACM Press
Full text available: pdf(617.70 KB) Additional Information: full citation, abstract, references, citings, index terms

We propose a new approach to securing self-organized mobile ad hoc networks. In this approach, security is achieved in a *fully self-organized* manner; by this we mean that the security system does not require any kind of certification authority or centralized server, even for the initialization phase. In our work, we were inspired by PGP [15] because its operation relies solely on the acquaintances between users. We show that the small-world phenomenon naturally emerges in the PGP system a ...

Keywords: PGP, public-key management, self-organization, small-world graphs

16 Integrating third party-certification with traditional computer education

Michael L. Nelson, David Rice

December 2001 **Journal of Computing Sciences in Colleges**, Volume 17 Issue 2
Publisher: Consortium for Computing Sciences in Colleges
Full text available: pdf(34.62 KB) Additional Information: full citation, abstract, references, index terms

Third-party, or independent certification has been receiving a lot of 'press' lately. Employers are looking for it, training agencies are pushing it, many educational institutions are looking at integrating it into their programs, and students are trying to figure out just how important it is and how to obtain it. This paper briefly considers the importance of third-party certification, and then looks at how it has been integrated into the Computer Information Technology curriculum at Internatio ...

17 Certifications - beat 'EM, join 'EM (or lose 'EM)?
John Mason
June 2003 **Journal of Computing Sciences in Colleges**, Volume 18 Issue 6
Publisher: Consortium for Computing Sciences in Colleges
Full text available: pdf(54.00 KB) Additional Information: full citation, references, citings, index terms

18 COCA: A secure distributed online certification authority
Lidong Zhou, Fred B. Schneider, Robbert Van Renesse
November 2002 **ACM Transactions on Computer Systems (TOCS)**, Volume 20 Issue 4
Publisher: ACM Press
Full text available: pdf(448.28 KB) Additional Information: full citation, abstract, references, citings, index terms

COCA is a fault-tolerant and secure online certification authority that has been built and deployed both in a local area network and in the Internet. Extremely weak assumptions characterize environments in which COCA's protocols execute correctly: no assumption is made about execution speed and message delivery delays; channels are expected to exhibit only intermittent reliability; and with $3t + 1$ COCA servers up to t may be faulty or compromised. COCA is the first system to integr ...

Keywords: Byzantine quorum systems, Certification authority, denial of service, proactive secret-sharing, public key infrastructure, threshold cryptography

19 A methodology for certification of modeling and simulation applications
Osman Balci
October 2001 **ACM Transactions on Modeling and Computer Simulation (TOMACS)**, Volume 11 Issue 4
Publisher: ACM Press
Full text available: pdf(2.44 MB) Additional Information: full citation, abstract, references, citings, index terms

Certification of modeling and simulation (M&S) applications poses significant technical challenges for M&S program managers, engineers, and practitioners. Certification is becoming increasingly more important as M&S applications are used more and more for military training, complex system design evaluation, M&S-based acquisition, problem solving, and critical decision making. Certification, a very complex process, involves the measurement and evaluation of hundreds of qualitative and quantitativ ...

Keywords: accreditation, certification, credibility assessment, evaluation, quality assessment, validation, verification

20 Predicting software quality for reuse certification

William M. Thomas, Deborah A. Cerino
November 1995 **Proceedings of the conference on TRI-Ada '95: Ada's role in global markets: solutions for a changing complex world TRI-Ada '95**
Publisher: ACM Press
Full text available: pdf(1.35 MB) Additional Information: full citation, references

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next

Terms used: **key self certificate application** Found **17** of **207,474**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window

Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 17 of 17

Relevance scale

1 Enhancement of digital signature with message recovery using self-certified public keys and its variants

Yi-Hwa Chen, Jinn-Ke Jan
July 2005 **ACM SIGOPS Operating Systems Review**, Volume 39 Issue 3
Publisher: ACM Press
Full text available: pdf(2.51 MB) Additional Information: full citation, abstract, references, index terms

In 2003, Tseng et al. proposed a self-certified public key signature with message recovery, which gives two advantages: one is that the signer's public key can simultaneously be authenticated in verifying the signature and the other one is that only the specified verifier can recover the message. Lately, Xie and YU proposed an attack to the Tseng et al.'s scheme under the cases: the specified verifier substitutes his secret key or two or more specified verifiers cooperatively forge the signer's ...

Keywords: authenticated encryption, forward secrecy, self-certified public key

2 At the forge: ebay web services

Reuven M. Lerner
August 2006 **Linux Journal**, Volume 2006 Issue 148
Publisher: Specialized Systems Consultants, Inc.
Full text available: html(1.40 MB) Additional Information: full citation, abstract, index terms

¿

3 A survey on peer-to-peer key management for mobile ad hoc networks

Johann Van Der Merwe, Dawoud Dawoud, Stephen McDonald
April 2007 **ACM Computing Surveys (CSUR)**, Volume 39 Issue 1
Publisher: ACM Press
Full text available: pdf(872.71 KB) Additional Information: full citation, abstract, references, index terms

The article reviews the most popular peer-to-peer key management protocols for mobile ad hoc networks (MANETs). The protocols are subdivided into groups based on their design strategy or main characteristic. The article discusses and provides comments on the strategy of each group separately. The discussions give insight into open research problems in the area of pairwise key management.

Keywords: Mobile ad hoc networks, pairwise key management, peer-to-peer key management, security

4 On the fly signatures based on factoring

Guillaume Poupard, Jacques Stern
November 1999 **Proceedings of the 6th ACM conference on Computer and communications security CCS '99**
Publisher: ACM Press

Full text available: pdf(786.71 KB) Additional Information: full citation, abstract, references, citings, index terms

In response to the current need for fast, secure and cheap public-key cryptography largely induced by the fast development of electronic commerce, we propose a new on the fly signature scheme, i.e. a scheme that requires very small on-line work for the signer It combines provable security based on the factorization problem, short public and secret keys, short transmission and minimal on-line computation. It is the first RSA-like signature scheme that can be used for both ef ...

5 Putting the U.S. standardization system into perspective: new insights

Bob Toth
December 1996 **StandardView**, Volume 4 Issue 4
Publisher: ACM Press
Full text available: pdf(172.91 KB) Additional Information: full citation, abstract, references, index terms

The odds are very high that an American attending an international standardization meeting or consulting in a foreign country will be asked about the U.S. standardization system. How is it organized? Who is responsible for developing standards? How many standards? Who sees to their implementation? What is the government's role? Why is there more than one standard for many commodities? Foreign engineers who are used to dealing with their national standards institute can be very critical of t ...

6 Measurement-based standards for future information technology systems

Shukri A. Wakid, Shirley M. Radack
March 1997 **StandardView**, Volume 5 Issue 1
Publisher: ACM Press
Full text available: pdf(73.69 KB) Additional Information: full citation, references, index terms, review

7 Secrecy by typing in security protocols

Martín Abadi
September 1999 **Journal of the ACM (JACM)**, Volume 46 Issue 5
Publisher: ACM Press

Full text available: pdf(265.35 KB) Additional Information: full citation, abstract, references, citings, index terms, review

We develop principles and rules for achieving secrecy properties in security protocols. Our approach is based on traditional classification techniques, and extends those techniques to handle concurrent processes that use shared-key cryptography. The rules have the form of typing rules for a basic concurrent language with cryptographic primitives, the spi calculus. They guarantee that, if a protocol typechecks, then it does not leak its secret inputs.

Keywords: cryptographic protocols, process calculi, secrecy properties

8 A wide-area Distribution Network for free software

Arno Bakker, Maarten Van Steen, Andrew S. Tanenbaum
August 2006 **ACM Transactions on Internet Technology (TOIT)**, Volume 6 Issue 3
Publisher: ACM Press
Full text available: pdf(215.08 KB) Additional Information: full citation, abstract, references, index terms

The Globe Distribution Network (GDN) is an application for the efficient, worldwide distribution of freely redistributable software packages. Distribution is made efficient by encapsulating the software into special distributed objects which efficiently replicate themselves near to the downloading clients. The Globe Distribution Network takes a novel, optimistic approach to stop the illegal distribution of copyrighted and illicit material via the network. Instead of having moderators check the p ...

Keywords: Distributed objects, copyright, file sharing, middleware, software distribution, traceable content, wide-area networks

9 On the security of some proxy blind signature schemes

Hung-Min Sun, Bin-Tsan Hsieh
January 2004 **Proceedings of the second workshop on Australasian information security, Data Mining and Web Intelligence, and Software Internationalisation - Volume 32 ACSW Frontiers '04**
Publisher: Australian Computer Society, Inc.
Full text available: pdf(171.20 KB) Additional Information: full citation, abstract, references, citings, index terms

A proxy blind signature scheme is a digital signature scheme which combines the properties of proxy signature and blind signature schemes. Recently, Tan et al. proposed two proxy blind signature schemes based on DLP and ECDLP respectively. Later, compared with Tan et al.'s scheme, Lal and Awasthi further proposed a more efficient proxy blind signature scheme. In this paper, we show that Tan et al.'s schemes do not satisfy the unforgeability and unlinkability properties. Moreover, we also point o ...

Keywords: crypt-analysis, cryptography, elliptic curve, proxy signature

10 Teaching secure communication protocols using a game representation

Leonard G. C. Hamey
January 2003 **Proceedings of the fifth Australasian conference on Computing education - Volume 20 ACE '03**
Publisher: Australian Computer Society, Inc.
Full text available: pdf(252.19 KB) Additional Information: full citation, abstract, references, index terms

The Security Protocol Game is a highly visual and interactive game for teaching secure data communication protocols. Students use the game to simulate protocols and explore possible attacks against them. The power of the game lies in the representation of secret and public key cryptography. Specifically, the game provides representations for plain text and encrypted messages, message digests, digital signatures and cryptographic keys. Using these representations, students can construct public ke ...

Keywords: PGP, blind signature, computer network, cryptography, digital signature, key exchange, man-in-the-middle attack, protocols, replay attack, secure communication

11 Programming languages for mobile code

Tommy Thorn

September 1997 **ACM Computing Surveys (CSUR)**, Volume 29 Issue 3
Publisher: ACM Press
Full text available: pdf(393.65 KB) Additional Information: full citation, abstract, references, citings, index terms, review

Sun's announcement of the programming language Java more that anything popularized the notion of mobile code, that is, programs traveling on a heterogeneous network and automatically executing upon arrival at the destination. We describe several classes of mobile code and extract their common characteristics, where security proves to be one of the major concerns. With these characteristics as reference points, we examine six representative languages proposed for mobile code. The conclusion ...

Keywords: Java, Limbo, Objective Caml, Obliq, Safe-Tcl, distribution, formal methods, mobile code, network programming, object orientation, portability, safety, security, telescript

12 CHI 96: a preview
Peter Stevens
January 1996 **ACM SIGCHI Bulletin**, Volume 28 Issue 1
Publisher: ACM Press
Full text available: pdf(1.58 MB) Additional Information: full citation, index terms

13 Unionization of professionals in data processing: an assessment of recent trends
Theodor D. Sterling
November 1982 **Communications of the ACM**, Volume 25 Issue 11
Publisher: ACM Press
Full text available: pdf(1.03 MB) Additional Information: full citation, abstract, references, index terms

The needs of management, unions, employees, and computer professionals combined with existing practices of Labor Relations Boards and the various divisions in the Departments of Labor have combined to create a unique array of social conflicts. At the root are management's interest in keeping many skills in data processing and computing out of bargaining units and the union's interest in including as many of these skills as possible. There is also conflict between past strategies guiding lab ...

Keywords: bargaining units, labor relations, software engineering, unionization of computer professionals

14 Security II: Neglect of information privacy instruction: a case of educational malpractice?
Victoria W. Romney, Gordon W. Romney
October 2004 **Proceedings of the 5th conference on Information technology education CITC5 '04**
Publisher: ACM Press
Full text available: pdf(128.22 KB) Additional Information: full citation, abstract, references, index terms

Not only should InformationTechnology (IT) Educators be knowledgeable regarding data privacy legislation but they should be teaching correct system and database design principles to IT students in order to ensure future application design compliance with international legislative trends. Perhaps the most contentious and serious issue facing IT practitioners in the world today is data privacy. Data Privacy impacts every aspect of IT from database and application design to privacy and use polic ...

Keywords: European union directive, Gramm-Leach-Bliley, HIPAA, IT education, data privacy, database design, legal issues, legislation

15 Editorial zone: How to lease the internet in your spare time

Nick Feamster, Lixin Gao, Jennifer Rexford
January 2007 **ACM SIGCOMM Computer Communication Review**, Volume 37 Issue 1
Publisher: ACM Press
Full text available: pdf(77.88 KB) Additional Information: full citation, abstract, references, index terms

Today's Internet Service Providers (ISPs) serve two roles: managing their network infrastructure and providing (arguably limited) services to end users. We argue that coupling these roles impedes the deployment of new protocols and architectures, and that the future Internet should support two separate entities: infrastructure providers (who manage the physical infrastructure) and service providers (who deploy network protocols and offer end-to-end services). We present a high-level design for C ...

16 Cryptology I: An efficient digital signature using self-certified public keys

Yuan Zhou, Zhenfu Cao, Rongxing Lu
November 2004 **Proceedings of the 3rd international conference on Information security InfoSecu '04**
Publisher: ACM Press
Full text available: pdf(318.70 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we first analyse the notion of self-certified public keys, which was first introduced by Girault [5], and then we extend it. After that, we will adopt the extended concept to propose a new signature scheme. The proposed scheme has a property that the signer's public key can simultaneously be authenticated in verifying the signature. Compared to earlier self-certified signature schemes, our scheme is more efficient and provable secure.

Keywords: RSA, factoring, self-certified cryptosystem, signature

17 Posters: Pride: peer-to-peer reputation infrastructure for decentralized environments

Prashant Dewan, Partha Dasgupta
May 2004 **Proceedings of the 13th international World Wide Web conference on Alternate track papers & posters WWW Alt. '04**
Publisher: ACM Press
Full text available: pdf(97.97 KB) Additional Information: full citation, abstract, references, citings, index terms

Peer-to-peer (P2P) networks use the fundamental assumption that the nodes in the network will cooperate and will not cheat. In the absence of any common goals shared by the nodes of a peer-to-peer network, external motivation to cooperate and be trustworthy is mandated. Digital Reputations can be used to inject trust among the nodes of a network. This paper presents PRIDE, a reputation system for decentralized peer-to-peer networks. PRIDE uses self-certification a scheme for identification of pe ...

Keywords: peer-to-peer, reputation systems, security

Results 1 - 17 of 17

Terms used: **self certificate public key** Found **54,686** of **207,474**

Sort results by: relevance
Display results: expanded form
Save results to a Binder
Search Tips
Open results in a new window
Try an Advanced Search
Try this search in The ACM Guide

Results 1 - 20 of 200 Result page: **1** 2 3 4 5 6 7 8 9 10 next
Best 200 shown Relevance scale

1 Cryptosystems & analysis: Self-Generated-Certificate Public Key Cryptography and certificateless signature/encryption scheme in the standard model: extended abstract
Joseph K. Liu, Man Ho Au, Willy Susilo
March 2007 **Proceedings of the 2nd ACM symposium on Information, computer and communications security ASIACCS '07**
Publisher: ACM Press
Full text available: pdf(444.72 KB) Additional Information: full citation, abstract, references

Certificateless Public Key Cryptography (CL-PKC) enjoys a number of features of Identity-Based Cryptography (IBC) while without having the problem of key escrow. However, it *does* suffer from an attack where the adversary, Carol, replaces Alice's public key by someone's public key so that Bob, who wants to send an encrypted message to Alice, uses Alice's identity and other's public key as the inputs to the encryption function. As a result, Alice cannot decrypt the message while Bob is u ...

Keywords: certificateless encryption, certificateless signature

2 Cryptosystems & analysis: Efficient and secure self-escrowed public-key infrastructures
Jaimee Brown, Juan M. Gonzalez Nieto, Colin Boyd
March 2007 **Proceedings of the 2nd ACM symposium on Information, computer and communications security ASIACCS '07**
Publisher: ACM Press
Full text available: pdf(470.52 KB) Additional Information: full citation, abstract, references

A self-escrowed public key infrastructure (SE-PKI) combines the usual functionality of a public-key infrastructure with the ability to recover private keys given some trap-door information. We present an additively homomorphic variant of an existing SE-PKI for ElGamal encryption. We also propose a new efficient SE-PKI based on the ElGamal and Okamoto-Uchiyama cryptosystems that is more efficient than the previous SE-PKI. This is the first SE-PKI that does not suffer from a key doubling proble ...

Keywords: key recovery, public-key infrastructures, self-escrowed encryption

3 Cryptology I: An efficient digital signature using self-certified public keys
Yuan Zhou, Zhenfu Cao, Rongxing Lu

November 2004 **Proceedings of the 3rd international conference on Information security InfoSecu '04**
Publisher: ACM Press
Full text available: pdf(318.70 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we first analyse the notion of self-certified public keys, which was first introduced by Girault [5], and then we extend it. After that, we will adopt the extended concept to propose a new signature scheme. The proposed scheme has a property that the signer's public key can simultaneously be authenticated in verifying the signature. Compared to earlier self-certified signature schemes, our scheme is more efficient and provable secure.

Keywords: RSA, factoring, self-certified cryptosystem, signature

4 Enhancement of digital signature with message recovery using self-certified public keys and its variants
Yi-Hwa Chen, Jinn-Ke Jan
July 2005 **ACM SIGOPS Operating Systems Review**, Volume 39 Issue 3
Publisher: ACM Press
Full text available: pdf(2.51 MB) Additional Information: full citation, abstract, references, index terms

In 2003, Tseng et al. proposed a self-certified public key signature with message recovery, which gives two advantages: one is that the signer's public key can simultaneously be authenticated in verifying the signature and the other one is that only the specified verifier can recover the message. Lately, Xie and YU proposed an attack to the Tseng et al.'s scheme under the cases: the specified verifier substitutes his secret key or two or more specified verifiers cooperatively forge the signer's ...

Keywords: authenticated encryption, forward secrecy, self-certified public key

5 A survey on peer-to-peer key management for mobile ad hoc networks
Johann Van Der Merwe, Dawoud Dawoud, Stephen McDonald
April 2007 **ACM Computing Surveys (CSUR)**, Volume 39 Issue 1
Publisher: ACM Press
Full text available: pdf(872.71 KB) Additional Information: full citation, abstract, references, index terms

The article reviews the most popular peer-to-peer key management protocols for mobile ad hoc networks (MANETs). The protocols are subdivided into groups based on their design strategy or main characteristic. The article discusses and provides comments on the strategy of each group separately. The discussions give insight into open research problems in the area of pairwise key management.

Keywords: Mobile ad hoc networks, pairwise key management, peer-to-peer key management, security

6 Large systems: Small worlds in security systems: an analysis of the PGP certificate graph
Srdjan Čapkun, Levente Buttyán, Jean-Pierre Hubaux
September 2002 **Proceedings of the 2002 workshop on New security paradigms NSPW '02**
Publisher: ACM Press

Full text available: pdf(617.70 KB) Additional Information: full citation, abstract, references, citings, index terms

We propose a new approach to securing self-organized mobile ad hoc networks. In this approach, security is achieved in a *fully self-organized* manner; by this we mean that the security system does not require any kind of certification authority or centralized server, even for the initialization phase. In our work, we were inspired by PGP [15] because its operation relies solely on the acquaintances between users. We show that the small-world phenomenon naturally emerges in the PGP system a ...

Keywords: PGP, public-key management, self-organization, small-world graphs

7 Separating key management from file system security

David Mazières, Michael Kaminsky, M. Frans Kaashoek, Emmett Witchel

December 1999 **ACM SIGOPS Operating Systems Review , Proceedings of the seventeenth ACM symposium on Operating systems principles SOSP '99**, Volume 33 Issue 5

Publisher: ACM Press

Full text available: pdf(1.77 MB) Additional Information: full citation, abstract, references, citings, index terms

No secure network file system has ever grown to span the Internet. Existing systems all lack adequate key management for security at a global scale. Given the diversity of the Internet, any particular mechanism a file system employs to manage keys will fail to support many types of use.We propose separating key management from file system security, letting the world share a single global file system no matter how individuals manage keys. We present SFS, a secure file system that avoids internal ...

8 Secret key distribution protocol using public key cryptography

Amit Parnerkar, Dennis Guster, Jayantha Herath

October 2003 **Journal of Computing Sciences in Colleges**, Volume 19 Issue 1

Publisher: Consortium for Computing Sciences in Colleges

Full text available: pdf(74.93 KB) Additional Information: full citation, abstract, references, index terms

This paper presents the description and analysis of a protocol, which uses hybrid crypto algorithms for key distribution. A triple DES with a 168-bit key is used to generate the secret key. This secret key is transferred with the help of public key cryptography. The authentication process is accomplished by using the message digest algorithm MD5. This protocol uses mutual authentication in which, both participants have to authenticate themselves via a third trusted certificate authority (CA). Th ...

9 A public-key based secure mobile IP

John Zao, Stephen Kent, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra

September 1997 **Proceedings of the 3rd annual ACM/IEEE international conference on Mobile computing and networking MobiCom '97**

Publisher: ACM Press

Full text available: pdf(1.95 MB) Additional Information: full citation, references, citings

10 A public-key based secure mobile IP

John Zao, Joshua Gahm, Gregory Troxel, Matthew Condell, Pam Helinek, Nina Yuan, Isidro Castineyra, Stephen Kent

October 1999 **Wireless Networks**, Volume 5 Issue 5

Publisher: Kluwer Academic Publishers

Full text available: pdf(255.65 KB) Additional Information: full citation, references, citings, index terms

11 Authentication: An approach to certificate path discovery in mobile Ad Hoc networks

He Huang, Shyhtsun Felix Wu
October 2003 **Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks SASN '03**
Publisher: ACM Press

Full text available: pdf(146.93 KB) Additional Information: full citation, abstract, references, citings, index terms

Public key certificates prove validity and authenticity of their ownership and possibly other properties. Certificate path discovery is the critical process for public key verification in hierarchical public key infrastructure (PKI) diagrams. This process is conventionally done in centralized public key management system such as central CA or directory. However, in an infrastructure-less environment, such as a mobile ad hoc network, no such central service is present due to network dynamics. Tha ...

Keywords: MANET, certificate path discovery, public key infrastructure, security

12 Identification control: Public key distribution through "cryptoIDs"

Trevor Perrin
August 2003 **Proceedings of the 2003 workshop on New security paradigms NSPW '03**
Publisher: ACM Press

Full text available: pdf(1.51 MB) Additional Information: full citation, abstract, references, citings, index terms

In this paper, we argue that person-to-person key distribution is best accomplished with a key-centric approach, instead of PKI: users should distribute public key fingerprints in the same way they distribute phone numbers, postal addresses, and the like. To make this work, fingerprints need to be *small*, so users can handle them easily; *multipurpose*, so only a single fingerprint is needed for each user; and *long-lived*, so fingerprints don't have to be frequently redistribute ...

Keywords: cryptoIDs, fingerprints, key distribution, key management, public key infrastructure

13 Special feature: Report on a working session on security in wireless ad hoc networks

Levente Buttyán, Jean-Pierre Hubaux
January 2003 **ACM SIGMOBILE Mobile Computing and Communications Review**, Volume 7 Issue 1
Publisher: ACM Press

Full text available: pdf(2.50 MB) Additional Information: full citation, references, citings

14 Security through the eyes of users: Hardening Web browsers against man-in-the-middle and eavesdropping attacks

Haidong Xia, José Carlos Brustoloni
May 2005 **Proceedings of the 14th international conference on World Wide Web WWW '05**
Publisher: ACM Press

Full text available: pdf(770.11 KB) Additional Information: full citation, abstract, references, index terms

Existing Web browsers handle security errors in a manner that often confuses users. In particular, when a user visits a secure site whose certificate the browser cannot verify, the browser typically allows the user to view and install the certificate and connect to the site despite the verification failure. However, few users understand the risk of man-in-the-middle attacks and the principles behind certificate-based authentication. We propose context-sensitive certificate verification (CSCV), w ...

Keywords: HTTPS, SSL, Web browser, certificate, eavesdropping attack, just-in-time instruction, man-in-the-middle attack, password, safe staging, well-in-advance instruction

15 A wide-area Distribution Network for free software

Arno Bakker, Maarten Van Steen, Andrew S. Tanenbaum
August 2006 **ACM Transactions on Internet Technology (TOIT)**, Volume 6 Issue 3
Publisher: ACM Press
Full text available: pdf(215.08 KB) Additional Information: full citation, abstract, references, index terms

The Globe Distribution Network (GDN) is an application for the efficient, worldwide distribution of freely redistributable software packages. Distribution is made efficient by encapsulating the software into special distributed objects which efficiently replicate themselves near to the downloading clients. The Globe Distribution Network takes a novel, optimistic approach to stop the illegal distribution of copyrighted and illicit material via the network. Instead of having moderators check the p ...

Keywords: Distributed objects, copyright, file sharing, middleware, software distribution, traceable content, wide-area networks

16 Escaping the evils of centralized control with self-certifying pathnames

David Mazières, M. Frans Kaashoek
September 1998 **Proceedings of the 8th ACM SIGOPS European workshop on Support for composing distributed applications EW 8**
Publisher: ACM Press
Full text available: pdf(671.29 KB) Additional Information: full citation, citings, index terms

17 A secure infrastructure for service discovery and access in pervasive computing

Jeffrey Undercoffer, Filip Perich, Andrej Cedilnik, Lalana Kagal, Anupam Joshi
April 2003 **Mobile Networks and Applications**, Volume 8 Issue 2
Publisher: Kluwer Academic Publishers
Full text available: pdf(308.34 KB) Additional Information: full citation, abstract, references, citings, index terms

Security is paramount to the success of pervasive computing environments. The system presented in this paper provides a communications and security infrastructure that goes far in advancing the goal of anywhere-anytime computing. Our work securely enables clients to access and utilize services in heterogeneous networks. We provide a service registration and discovery mechanism implemented through a hierarchy of service management. The system is built upon a simplified Public Key Infrastructure t ...

Keywords: distributed services, extensible markup language, pervasive computing, security, smartcards

18 Security: Fast authenticated key establishment protocols for self-organizing sensor

networks
Qiang Huang, Johnas Cukier, Hisashi Kobayashi, Bede Liu, Jinyun Zhang
September 2003 **Proceedings of the 2nd ACM international conference on Wireless sensor networks and applications WSNA '03**
Publisher: ACM Press
Full text available: pdf(303.05 KB) Additional Information: full citation, abstract, references, index terms

In this paper, we consider efficient authenticated key establishment protocols between a sensor and a security manager in a self-organizing sensor network. We propose a hybrid authenticated key establishment scheme, which exploits the difference in capabilities between security managers and sensors, and put the cryptographic burden where the resources are less constrained. The hybrid scheme reduces the high cost public-key operations at the sensor side and replaces them with efficient symmetric- ...

Keywords: elliptic curve cryptography, key establishment, security, sensor network

19 Secure communications between bandwidth brokers
Bu-Sung Lee, Wing-Keong Woo, Chai-Kiat Yeo, Teck-Meng Lim, Bee-Hwa Lim, Yuxiong He, Jie Song
January 2004 **ACM SIGOPS Operating Systems Review**, Volume 38 Issue 1
Publisher: ACM Press
Full text available: pdf(922.33 KB) Additional Information: full citation, abstract, references

In the Differentiated Services (DiffServ) architecture, each domain has a Bandwidth Broker to provide the resources management, primarily bandwidth reservation. In a multi-domain environment, Simple Inter-domain Bandwidth Broker Signaling (SIBBS) protocol is proposed for the inter-domain communication protocol proposed for bandwidth broker communication. Since the information exchanged between BBs are sensitive in sense of Service Level Agreement (SLA), the communications between the inter-domai ...

Keywords: Bandwidth Broker, Public Key Infrastructure, Simple Inter-domain Bandwidth Broker Signaling

20 Extending cryptographic logics of belief to key agreement protocols
Paul van Oorschot
December 1993 **Proceedings of the 1st ACM conference on Computer and communications security CCS '93**
Publisher: ACM Press
Full text available: pdf(1.35 MB) Additional Information: full citation, abstract, references, citings, index terms

The authentication logic of Burrows, Abadi and Needham (BAN) provided an important step towards rigourous analysis of authentication protocols, and has motivated several subsequent refinements. We propose extensions to BAN-like logics which facilitate, for the first time, examination of public-key based authenticated key establishment protocols in which both parties contribute to the derived key (i.e. key agreement protocols). Attention is focussed on six distinct generic goals for authenti ...